(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平11－298470

(43)公開日　平成11年(1999)10月29日

(51)Int.Cl.[6]	識別記号	FI	
H04L 9/08		H04L 9/00	601E
9/10			601B
9/32			601A
			621A
			675D

審査請求　未請求　請求項の数14　OL　（全９頁）

(21)出願番号　特願平10－106437

(22)出願日　平成10年(1998)４月16日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　山▲崎▼　正嵩
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

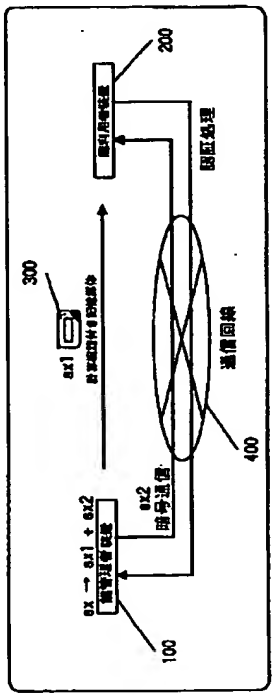
(72)発明者　西岡　玄次
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　富田　和子

(54)【発明の名称】　鍵の配布方法およびシステム

(57)【要約】
【課題】鍵管理者が鍵利用者に秘密鍵情報を配布する際、当該秘密鍵情報が不正者に横取りされる可能性を減少させる。
【解決手段】鍵管理者装置１００は、秘密鍵Ｓを秘密情報Ｓ１、Ｓ２に分割し、Ｓ１を記憶媒体３００に格納して鍵利用者にオフラインで配布する。鍵利用者装置２００は、配布された記憶媒体に格納されている秘密情報Ｓ１と予め鍵利用者に付与された識別情報ＩＤとを用いて、鍵管理者装置１００との間で認証処理を行う。認証された場合、鍵管理者装置１００は、残りの秘密情報Ｓ２を、通信回線４００を介して、オンライン送信する。鍵利用者装置２００は、オフライン配布された秘密情報Ｓ１とオンライン送信された秘密情報Ｓ２とを基に秘密鍵Ｓを復元する。

図1



1

【特許請求の範囲】

【請求項1】暗号通信に用いる鍵の配布方法であって、

鍵管理者の装置において、

秘密鍵Ｓを作成し、当該秘密鍵Ｓを少なくとも2つの秘密情報Ｓ1～Ｓｎ（ｎ≧2）に分割する第1のステップと、

前記第1のステップで得た秘密情報Ｓ1～Ｓｎのうちの少なくとも1つの秘密情報Ｓｉ（1≦ｉ≦ｎ）をオフラインで鍵利用者に配布する第2のステップと、

鍵利用者の装置において、

前記第2のステップによりオフラインで配布された秘密情報Ｓｉと、鍵管理者により予め付与された識別情報ＩＤとを基に、認証情報ＡＳを作成し、当該認証情報ＡＳを鍵管理者の装置に送信する第3のステップと、

鍵管理者の装置において、

前記第3のステップにより送信された認証情報ＡＳに基づいて、鍵利用者の認証処理を行う第4のステップと、

前記第4のステップにて鍵利用者が認証された場合、当該鍵利用者の装置に、前記第1のステップで得た秘密情報Ｓ1～Ｓｎのうち、前記第2のステップで当該鍵利用者にオフラインで配布した秘密情報Ｓｉ以外の秘密情報を送信する第5のステップと、

鍵利用者の装置において、

前記第5のステップにより送信された、秘密情報Ｓｉ以外の秘密情報Ｓ1～Ｓｎと、前記第2のステップによりオフラインで配布された秘密情報Ｓｉとを基に、前記秘密鍵Ｓを作成する第6のステップと、を備えることを特徴とする鍵の配布方法。

【請求項2】請求項1記載の鍵の配布方法であって、

前記第5のステップは、前記第4のステップにて鍵利用者が認証された場合、当該鍵利用者の装置に、前記第1のステップで得た秘密情報Ｓ1～Ｓｎのうち、前記第2のステップで当該鍵利用者にオフラインで配布した秘密情報Ｓｉ以外の秘密情報を、前記秘密情報Ｓｉを鍵として暗号化して送信するものであり、

前記第6のステップは、前記第5のステップにより送信された、秘密情報Ｓｉ以外の暗号化された秘密情報Ｓ1～Ｓｎを、前記秘密情報Ｓｉを鍵として復号化し、復号結果と前記秘密情報Ｓｉとを基に、前記秘密鍵Ｓを作成するものであることを特徴とする鍵の配布方法。

【請求項3】請求項1または2記載の鍵の配布方法であって、

鍵利用者の装置において、

前記第6のステップにより復元された秘密鍵Ｓを基に、認証情報ＡＳ´を作成し、当該認証情報ＡＳ´を鍵管理者の装置に送信する第7のステップと、

鍵管理者の装置において、

前記第7のステップにより送信された認証情報ＡＳ´に基づいて、鍵利用者の認証処理を行う第8のステップと、

2

鍵管理者の装置および／または鍵利用者の装置において前記第8のステップにて鍵利用者が認証された場合に、当該鍵利用者の、前記秘密鍵Ｓを用いた暗号通信に対する登録料金の課金処理を行う第9のステップを、さらに備えることを特徴とする鍵の配布方法。

【請求項4】鍵を生成する鍵管理者装置と、当該鍵管理者装置が生成した鍵を用いて暗号通信を行う鍵利用者装置と、でなる鍵の配布システムであって、

前記鍵管理者装置は、

秘密鍵Ｓを作成し、当該秘密鍵Ｓを少なくとも2つの秘密情報Ｓ1～Ｓｎ（ｎ≧2）に分割する鍵生成手段と、

前記鍵生成手段で得た秘密情報Ｓ1～Ｓｎのうちの少なくとも1つの秘密情報Ｓｉ（1≦ｉ≦ｎ）を記憶媒体に記憶する記憶手段と、

前記鍵利用者装置から送信された認証情報ＡＳを受信する第1の受信手段と、

前記受信手段で受信した認証情報ＡＳに基づいて、鍵利用者の認証処理を行う認証手段と、

前記認証手段により鍵利用者が認証された場合、前記鍵利用者装置に、前記鍵生成手段で得た秘密情報Ｓ1～Ｓｎのうち、前記記憶手段で記憶媒体に記憶した秘密情報Ｓｉ以外の秘密情報を送信する第1の送信手段と、を備え、

前記鍵利用者装置は、

前記鍵管理者装置により秘密情報Ｓｉが記憶された記憶媒体から、前記秘密情報Ｓｉを読み出す読出手段と、

前記読出手段により読み出された秘密情報Ｓｉと、鍵管理者により予め付与された識別情報ＩＤとを基に、認証情報ＡＳを作成する認証情報作成手段と、

前記認証情報作成手段により作成された認証情報ＡＳを前記鍵管理者装置に送信する第2の送信手段と、

前記鍵管理者装置により送信された、秘密情報Ｓｉ以外の秘密情報Ｓ1～Ｓｎを受信する第2の受信手段と、

前記読出手段により読み出された秘密情報Ｓｉと、前記第2の受信手段で受信した、秘密情報Ｓｉ以外の秘密情報Ｓ1～Ｓｎとを基に、前記鍵管理装置が生成した秘密鍵Ｓを復元する鍵復元手段と、を備えることを特徴とする鍵の配布システム。

【請求項5】鍵を生成する鍵管理者装置と、当該鍵管理者装置が生成した鍵を用いて暗号通信を行う鍵利用者装置と、計算機能付き記憶媒体と、でなる鍵の配布システムであって、

前記鍵管理者装置は、

秘密鍵Ｓを作成し、当該秘密鍵Ｓを少なくとも2つの秘密情報Ｓ1～Ｓｎ（ｎ≧2）に分割する鍵生成手段と、

前記鍵生成手段で得た秘密情報Ｓ1～Ｓｎのうちの少なくとも1つの秘密情報Ｓｉ（1≦ｉ≦ｎ）を、前記計算機能付き記憶媒体に記憶する記憶手段と、

前記鍵利用者装置から送信された認証情報ＡＳを受信する第1の受信手段と、

前記受信手段で受信した認証情報ＡＳに基づいて、鍵利用者の認証処理を行う認証手段と、
前記認証手段により鍵利用者が認証された場合、前記鍵利用者装置に、前記鍵生成手段で得た秘密情報Ｓ１～Ｓｎのうち、前記記憶手段で前記計算機能付き記憶媒体に記憶した秘密情報Ｓｉ以外の秘密情報を送信する第１の送信手段と、を備え、
前記鍵利用者装置は、
前記計算機能付き記憶媒体を接続する接続手段と、
前記接続手段により接続された前記計算機能付き記憶媒体から出力された認証情報ＡＳを前記鍵管理者装置に送信する第２の送信手段と、
前記鍵管理者装置から送信された、秘密情報Ｓｉ以外の秘密情報Ｓ１～Ｓｎを受信して、前記接続手段により接続された前記計算機能付き記憶媒体に出力する第２の受信手段と、を備え、
前記計算機能付き記憶媒体は、
記憶している秘密情報Ｓｉと鍵管理者により予め付与された識別情報ＩＤとをを基に、認証情報ＡＳを作成し、自己が接続している前記鍵利用者装置に出力する認証情報作成手段と、
記憶している秘密情報Ｓｉと、自己が接続している前記鍵利用者装置から出力された、秘密情報Ｓｉ以外の秘密情報Ｓ１～Ｓｎとを基に、前記鍵管理装置が生成した秘密鍵Ｓを復元する鍵復元手段と、を備えることを特徴とする鍵の配布システム。
【請求項６】暗号通信を行う鍵利用者に鍵を配布する情報処理装置であって、
秘密鍵Ｓを作成し、当該秘密鍵Ｓを少なくとも２つの秘密情報Ｓ１～Ｓｎ（ｎ≧２）に分割する鍵生成手段と、
前記鍵生成手段で得た秘密情報Ｓ１～Ｓｎのうちの少なくとも１つの秘密情報Ｓｉ（１≦ｉ≦ｎ）を記憶媒体に記憶する記憶手段と、
鍵利用者の装置から送信された、秘密情報Ｓｉと当該鍵利用者に予め付与した識別情報とを基に作成された認証情報ＡＳを受信する受信手段と、
前記受信手段で受信した認証情報ＡＳに基づいて、鍵利用者の認証処理を行う認証手段と、
前記認証手段により鍵利用者が認証された場合、当該鍵利用者の装置に、前記鍵生成手段で得た秘密情報Ｓ１～Ｓｎのうち、前記記憶手段で記憶媒体に記憶した秘密情報Ｓｉ以外の秘密情報を送信する送信手段と、を備えることを特徴とする情報処理装置。
【請求項７】請求項６記載の情報処理装置であって、
前記認証手段により鍵利用者が認証された場合、前記鍵生成手段で得た秘密情報Ｓ１～Ｓｎのうち、前記記憶手段で記憶媒体に記憶した秘密情報Ｓｉ以外の秘密情報を、前記秘密情報Ｓｉを鍵として暗号化し、前記送信手段に出力する暗号化手段をさらに備えることを特徴とする情報処理装置。

【請求項８】請求項６または７記載の情報処理装置であって、
前記受信手段は、鍵利用者の装置から送信された、秘密鍵Ｓを基に作成された認証情報ＡＳ´を受信するものであり、
前記認証手段は、前記受信手段で受信した認証情報ＡＳ´に基づいて、鍵利用者の認証処理を行うものであり、
前記認証手段により、認証情報ＡＳ´に基づいて鍵利用者が認証された場合に、当該鍵利用者の、前記秘密鍵Ｓを用いた暗号通信に対する登録料金を特定する情報を記憶する課金手段を、さらに備えることを特徴とする情報処理装置。
【請求項９】鍵管理者の装置にて、秘密鍵Ｓを少なくとも２つに分割することで得られた秘密情報Ｓ１～Ｓｎ（ｎ≧２）を基に鍵を復元する情報処理装置であって、
鍵管理者から配布された記憶媒体に記憶された秘密情報Ｓｉ（１≦ｉ≦ｎ)を読み出す読出手段と、
前記読出手段により読み出された秘密情報Ｓｉと、鍵管理者により予め付与された識別情報ＩＤとを基に、認証情報ＡＳを作成する認証情報作成手段と、
前記認証情報作成手段により作成された認証情報ＡＳを鍵管理者の装置に送信する送信手段と、
鍵管理者の装置から送信された、秘密情報Ｓｉ以外の秘密情報Ｓ１～Ｓｎを受信する受信手段と、
前記読出手段により読み出された秘密情報Ｓｉと、前記受信手段で受信した、秘密情報Ｓｉ以外の秘密情報Ｓ１～Ｓｎとを基に、秘密鍵Ｓを復元する鍵復元手段と、を備えることを特徴とする情報処理装置。
【請求項１０】請求項９記載の情報処理装置であって、
鍵管理者の装置から送信された、秘密情報Ｓｉ以外の秘密情報Ｓ１～Ｓｎは、秘密情報Ｓｉを鍵として暗号化されたものであり、
前記受信手段で受信した、秘密情報Ｓｉ以外の暗号化された秘密情報Ｓ１～Ｓｎを、前記読出手段により読み出された秘密情報Ｓｉを鍵として復号化し、前記鍵復元手段に出力する復号化手段をさらに備えることを特徴とする情報処理装置。
【請求項１１】請求項９または１０記載の情報処理装置であって、
前記認証情報作成手段は、前記鍵復元手段により復元された秘密鍵Ｓを基に、認証情報ＡＳ´を作成するものであり、
前記送信手段は、前記認証情報作成手段により作成された認証情報ＡＳ´を鍵管理者の装置に送信するものであり、
鍵管理者の装置にて、前記認証情報ＡＳ´により鍵利用者が認証された場合に、当該鍵利用者の、前記秘密鍵Ｓを用いた暗号通信に対する登録料金を特定する情報を記憶する課金手段を、さらに備えることを特徴とする情報処理装置。

5　　6

【請求項12】鍵管理者の装置にて、秘密鍵Sを少なくとも2つに分割することで得られた秘密情報S1～Sn（n≧2）を基に鍵を復元する、当該鍵を用いて暗号通信を行う鍵利用者の装置に挿抜可能に構成された計算機能付き記憶媒体であって、
記憶している秘密情報Si（1≦i≦n）と、鍵管理者により予め付与された識別情報IDとを基に認証情報ASを作成し、自己が接続している鍵利用者の装置を介して、鍵管理者の装置に送信する認証情報作成手段と、
鍵管理者の装置により記憶された秘密情報Siと、自己が接続している鍵利用者の装置を介して受け取った、鍵管理者の装置が送信した秘密情報Si以外の秘密情報S1～Snとを基に、前記秘密鍵Sを復元する鍵復元手段と、を備えることを特徴とする計算機能付き記憶媒体。
【請求項13】請求項12記載の計算機能付き記憶媒体であって、
鍵管理者の装置から送信された、秘密情報Si以外の秘密情報S1～Snは、秘密情報Siを鍵として暗号化されたものであり、
自己が接続している前記鍵利用者装置が受信した、秘密情報Si以外の暗号化された秘密情報S1～Snを、記憶している秘密情報Siを鍵として復号化し、前記鍵復元手段に出力する復号化手段をさらに備えることを特徴とする計算機能付き記憶媒体。
【請求項14】請求項12または13記載の計算機能付き記憶媒体であって、
前記認証情報作成手段は、前記鍵復元手段により復元された秘密鍵Sを基に、認証情報AS´を作成し、自己が接続している鍵利用者の装置を介して、鍵管理者の装置に送信するものであり、
鍵管理者の装置にて、前記認証情報AS´により鍵利用者が認証された場合に、当該鍵利用者の、前記秘密鍵Sを用いた暗号通信に対する登録料金を特定する情報を記憶する課金手段を、さらに備えることを特徴とする計算機能付き記憶媒体。
【発明の詳細な説明】
【0001】
【発明の属する分野】本発明は、暗号通信に用いる鍵を鍵利用者（たとえば、暗号データの受信者）に配布する技術に関する。
【0002】
【従来の技術】一般に、大量のデータを暗号通信する場合、秘密鍵暗号が用いられている。秘密鍵暗号では、送信者と受信者との間で共通の鍵（共通鍵）を持つ必要がある。共通鍵の配送方法としては、コピー鍵方式、個別鍵方式等があるが、いずれの場合においても、秘密鍵情報を受信者に配布しなければならない。従来は、たとえば、ICカード等に秘密鍵情報を搭載して、受信者にオフラインで配布したり、あるいは、暗号通信等により受信者に秘密鍵情報を送信することで、秘密鍵情報を受信者に配布している。
【0003】
【発明が解決しようとする課題】しかしながら、秘密鍵情報をICカード等に搭載してオフラインで配布する方法では、不正者がこの記憶媒体を盗用し、正規の受信者になりすます可能性が考えられる。また、秘密鍵情報を暗号通信等により送信する方法では、不正者が秘密鍵情報を盗聴・解読し、正規の受信者になりすます可能性が考えられる。
【0004】本発明は、上記事情に鑑みてなされたものであり、本発明の目的は、秘密鍵情報を配布する際に、当該秘密鍵情報が不正者に横取りされる可能性を減少させ、暗号通信のセキュリティを向上させることにある。
【0005】
【課題を解決するための手段】上記課題を解決するために、本発明は、暗号通信に用いる鍵の配布方法であって、鍵管理者の装置において、秘密鍵Sを作成し、当該秘密鍵Sを少なくとも2つの秘密情報S1～Sn（n≧2）に分割する第1のステップと、前記第1のステップで得た秘密情報S1～Snのうちの少なくとも1つの秘密情報Si（1≦i≦n）をオフラインで鍵利用者に配布する第2のステップと、鍵利用者の装置において、前記第2のステップによりオフラインで配布された秘密情報Siと、鍵管理者により予め付与された識別情報IDとを基に、認証情報ASを作成し、当該認証情報ASを鍵管理者の装置に送信する第3のステップと、鍵管理者の装置において、前記第3のステップにより送信された認証情報ASに基づいて、鍵利用者の認証処理を行う第4のステップと、前記第4のステップにて鍵利用者が認証された場合、当該鍵利用者の装置に、前記第1のステップで得た秘密情報S1～Snのうち、前記第2のステップで当該鍵利用者にオフラインで配布した秘密情報Si以外の秘密情報を送信する第5のステップと、鍵利用者の装置において、前記第5のステップにより送信された、秘密情報Si以外の秘密情報S1～Snと、前記第2のステップによりオフラインで配布された秘密情報Siとを基に、前記秘密鍵Sを作成する第6のステップと、を備えることを特徴とする。
【0006】本発明によれば、鍵管理者は、秘密鍵Sを複数の秘密情報S1～Snに分割し、そのうちの少なくとも1つの秘密情報Siを記憶媒体（ICカード等の計算機能付き記憶媒体を含む）に搭載してオフラインで鍵利用者に配布している。そして、残りについては、秘密情報Siおよび鍵利用者に付与された識別情報IDを基に作成した認証情報ASにより鍵利用者を認証した場合にのみ、当該鍵利用者にオンラインで送信するようにしている。
【0007】このようにすることで、たとえ、オフラインで配布した記憶媒体が不正者に盗用されたとしても、それだけでは、不正者は、秘密鍵Sを復元するのに必要

なすべての秘密情報Ｓ１～Ｓｎを取得したことにならない。同様に、オンラインで送信した秘密情報が不正者に盗聴されたとしても、それだけでは、不正者は、秘密鍵Ｓを復元するのに必要なすべての秘密情報Ｓ１～Ｓｎを取得したことにならない。このため、秘密鍵情報を配布する際に、当該秘密鍵情報が不正者に横取りされる可能性を減少させることができ、ひいては、暗号通信のセキュリティを向上させることができる。

【０００８】なお、本発明において、第５のステップは、第４のステップにて鍵利用者が認証された場合、当該鍵利用者の装置に、前記第１のステップで得た秘密情報Ｓ１～Ｓｎのうち、前記第２のステップで当該鍵利用者にオフラインで配布した秘密情報Ｓｉ以外の秘密情報を、前記秘密情報Ｓｉを鍵として暗号化して送信するものであり、第６のステップは、第５のステップにより送信された、秘密情報Ｓｉ以外の暗号化された秘密情報Ｓ１～Ｓｎを、前記秘密情報Ｓｉを鍵として復号化し、復号結果と前記秘密情報Ｓｉとを基に、前記秘密鍵Ｓを作成するものでもよい。

【０００９】このようにすることで、秘密情報Ｓｉ以外の秘密情報Ｓ１～Ｓｎをオンラインで送信する際のセキュリティをさらに向上させることができる。

【００１０】

【発明の実施の形態】以下に、本発明の一実施形態について説明する。

【００１１】図１は、本発明の一実施形態である秘密鍵配布方法が適用されたシステムの概略図である。

【００１２】図示するように、本実施形態方法は、相互に通信回線400で接続された鍵管理者装置１００および鍵利用者装置２００と、鍵管理者装置１００および鍵利用者装置２００に挿抜可能に構成された計算機能付き記憶媒体３００と、を含んで構成されるシステムにおいて実施される。

【００１３】図２に、鍵管理者装置１００の概略機能構成を示す。

【００１４】図示するように、鍵管理者装置１００は、乱数生成部１０１と、演算部１０２と、暗復号化部１０３と、認証部１０４と、課金部１０５と、メモリ１０６と、通信部１０７と、で構成される。これらの機能構成は、コンピュータにおいて、各機能を実現するための手順が記述されたプログラムを実行することにより、ソフトウエア的に実現されるものでもよいし、あるいは、各機能を実現するロジックを組むことによりハードウエア的に実現されるようにしてもよい。ソフトウエア的に実現される場合は、各機能を実現するための手順が記述されたプログラムを、ＣＤ－ＲＯＭ等の記憶媒体に格納して、コンピュータに供給するようにしてもよい。

【００１５】なお、鍵管理者装置１００には、オフラインで鍵利用者に配布する計算機能付き記憶媒体３００を接続するための機構が設けられている。

【００１６】図３に、鍵利用者装置２００の概略機能構成を示す。

【００１７】図示するように、鍵利用者装置２００は、乱数生成部２０１と、素数生成部２０２と、演算部２０３と、暗復号化部２０４と、メモリ２０５と、通信部２０６と、で構成される。これらの機能構成は、鍵管理者装置１００と同様、コンピュータにおいて、各機能を実現するため手順が記述されたプログラムを実行することにより、ソフトウエア的に実現されるものでもよいし、あるいは、各機能を実現するロジックを組むことによりハードウエア的に実現されるようにしてもよい。ソフトウエア的に実現される場合は、各機能を実現するための手順が記述されたプログラムを、ＣＤ－ＲＯＭ等の記憶媒体に格納して、コンピュータに供給するようにしてもよい。

【００１８】なお、鍵利用者装置２００は、オフラインで鍵管理者から配布された計算機能付き記憶媒体３００を接続するための機構が設けられている。

【００１９】図４に、計算機能付き記憶媒体３００の概略機能構成を示す。

【００２０】図示するように、計算機能付き記憶媒体３００は、暗復号化部３０１と、演算部３０２と、メモリ３０３と、で構成される。これらの機能構成は、ＩＣカードにおいて、各機能を実現するため手順が記述されたプログラムを実行することにより、ソフトウエア的に実現されるものでもよいし、あるいは、各機能を実現するロジックを組むことによりハードウエア的に実現されるようにしてもよい。

【００２１】次に、上記説明したシステムにおいて実施される、本発明の第一実施形態である秘密鍵配布方法について説明する。

【００２２】まず、鍵管理者装置１００は、鍵管理者の指示にしたがい、乱数生成部１０１によって、乱数Ｓを生成し、これを鍵利用者の秘密鍵とする。その後、演算部１０２により秘密鍵Ｓを秘密情報Ｓ１、Ｓ２に分割し、秘密鍵Ｓ、および秘密情報Ｓ１、Ｓ２をメモリ１０６に格納する。次に、鍵管理者装置１００は、メモリ１０６から秘密情報Ｓ１を取り出し、これを鍵管理者装置１００に接続された計算機能付き記憶媒体３００内のメモリ３０３に格納する。

【００２３】鍵管理者は、秘密情報Ｓ１が格納された計算機能付き記憶媒体３００を対象となる鍵利用者にオフラインで配布する。

【００２４】秘密情報Ｓ１が格納された計算機能付き記憶媒体３００を受け取った鍵利用者は、これを鍵利用者装置２００に接続する。

【００２５】鍵利用者装置２００は、鍵利用者の指示にしたがい、計算機能付き記憶媒体３００から秘密情報Ｓ１を取り出し、秘密情報Ｓ１と鍵管理者により予め付与された当該鍵利用者の識別情報ＩＤとを使って、鍵管理

者装置１００との間で認証処理を行う。

【００２６】認証処理には様々な方法があるが、ここでは、一例として、ＲＳＡ署名法を用いた場合とエルガマル署名法を用いた場合とについて、説明する。

【００２７】まず、ＲＳＡ署名法を用いた場合について説明する。

数1

・秘密情報　p,q：素数

・署名鍵　$(d,n), d\in\mathbb{Z}, n=pq$

・検証鍵　$(e,n), e\in\mathbb{Z}, n=pq$　　…(数1)

【００２８】鍵利用者装置２００は、鍵利用者の指示にしたがい、予め以下の情報を、乱数生成部２０１、素数生成部２０２および演算部２０３を用いて作成し、メモリ２０５に格納しておく。

【００２９】

【数1】

【００３０】ここで、署名鍵は秘密、検証鍵は公開とする。鍵利用者装置２００は、署名鍵と、鍵利用者が入力した、鍵管理者により予め付与された当該鍵利用者の識別情報ＩＤとを計算機能付き記憶媒体３００に出力する。これを受けて、計算機能付き記憶媒体３００は、演算部３０２により、

【００３１】

【数2】

数2

$$AS = S'^{d} \pmod{n} \qquad \cdots(数2)$$

【００３２】から認証情報ＡＳを計算する。ここで、Ｓ'は、秘密情報Ｓ１と識別情報ＩＤとを入力とする所定の関数の値（たとえば、ハッシュ値）である。次に、計算機能付き記憶媒体３００は、認証情報ＡＳを鍵利用者装置２００に出力する。これを受けて、鍵利用者装置２００は、通信部２０６により、認証情報ＡＳを、通信回線４００を介して、鍵管理者装置１００に送信する。

【００３３】鍵管理者装置１００は、通信部１０７により認証情報ＡＳを受信すると、認証部１０４により、

【００３４】

【数3】

数3

$$S' = AS^{e} \pmod{n} \qquad \cdots(数3)$$

【００３５】が成立するか否かを検証し、成立すれば、認証情報ＡＳを送ってきた鍵利用者装置２００の鍵利用者が正当な鍵利用者であると認証する。なお、鍵管理者装置１００は、鍵利用者に付与した識別情報ＩＤを、当該鍵利用者にオフラインで配布した計算機能付き記憶媒体３００に格納された秘密情報Ｓ１と対応付けて、メモリ１０６に格納しているものとする。

【００３６】次に、エルガマル署名法を用いた場合について説明する。

【００３７】鍵利用者装置２００は、鍵利用者の指示にしたがい、素数生成部２０２により素数ｐを生成し、演※算部２０２により、

【００３８】

【数4】

数4

$$\mathrm{ord}_{p}(\alpha)=p-1 \qquad \cdots(数4)$$

【００３９】を満たすαを作成する。そして、作成したαおよび素数ｐを計算機能付き記憶媒体３００に出力する。これを受けて、計算機能付き記憶媒体３００は、演算部３０２により、

【００４０】

【数5】

数5

$$y = \alpha^{s'} \pmod{p} \qquad \cdots(数5)$$

【００４１】を満たすｙを計算し、署名鍵を（ｘ，α，ｐ）、検証鍵を（ｙ，α，ｐ）とする。ここで、Ｓ'は、秘密情報Ｓ１と識別情報ＩＤとを入力とする所定の関数の値（たとえば、ハッシュ値）である。

【００４２】次に、鍵利用者装置２００は、ｐ－１と互いに素な乱数ｋを乱数生成部２０１により作成し、

【００４３】

【数6】

数6

$$r = \alpha^{k} \pmod{p} \qquad \cdots(数6)$$

【００４４】を満たすｒを計算する。さらに、適当なメッセージｍを乱数生成部２０１により生成し、ｒ、ｋとともに計算機能付き記憶媒体３００に出力する。これを受けて、計算機能付き記憶媒体３００は、演算部３０２により、

【００４５】

【数7】

数7

$$t = (m - S'r)k^{-1} \pmod{p-1} \quad \cdots(数7)$$

【0046】を満たすtを計算する。そして、（r，t）をメッセージmに対する署名とし、メッセージm，署名（r，s）を、鍵利用者装置２００に出力する。これを受けて、鍵利用者装置２００は、通信部２０６より、メッセージm，署名（r，s）を、通信回線４００を介して、鍵管理者装置１００に送信する。

【0047】鍵管理者装置１００は、メッセージm，署名（r，s）を受け取ると、認証部１０４により、

【0048】

【数8】

数8

$$\alpha^m = y^r r^t \pmod{p} \quad \cdots(数8)$$

【0049】が成立するか否かを検証し、成立すれば、メッセージm，署名（r，s）を送ってきた鍵利用者装置２００の鍵利用者が正当な鍵利用者であると認証する。なお、鍵管理者装置１００は、鍵利用者に付与した識別情報ＩＤを、当該鍵利用者にオフラインで配布した計算機能付き記憶媒体３００に格納された秘密情報Ｓ１と対応付けて、メモリ１０６に格納しているものとする。

【0050】以上説明した認証処理により、鍵利用者が認証されると、鍵管理者装置１００は、暗復号化部１０３により、秘密情報Ｓ１を鍵として秘密情報Ｓ２を暗号化する。そして、通信部１０７により、暗号化された秘密情報Ｓ２を、通信回線４００を介して、鍵利用者装置２００に送信する。

【0051】鍵利用者装置２００は、暗号化された秘密情報Ｓ２を受け取ると、これを計算機能付き記憶媒体３００に出力する。これを受けて、計算機能付き記憶媒体３００は、暗復号化部３０１により、暗号化された秘密情報Ｓ２を、秘密情報Ｓ１を鍵として復号化し、メモリ３０３に格納する。さらに、演算装置３０２により、復号化された秘密情報Ｓ２、および秘密情報Ｓ１を基に、秘密鍵Ｓを復元し、メモリ３０３に格納する。

【0052】次に、鍵利用者装置２００は、鍵利用者の指示にしたがい、計算機能付き記憶媒体３００から秘密鍵Ｓを取り出し、この秘密鍵Ｓを使って、鍵管理者装置１００との間で、上記と同様の手順により認証処理を行う。

【0053】なお、ＲＳＡ署名法を用いる場合は、上記の（数２）、（数３）において、Ｓ´の代わりに秘密鍵Ｓを用いればよい。また、エルガマル署名法を用いる場合には、上記の（数５）、（数７）において、Ｓ´の代わりに秘密鍵Ｓを用いればよい。

＊【0054】鍵利用者が認証されると、鍵管理者装置１００は、課金部１０５により、当該鍵利用者の、秘密鍵Ｓを用いた暗号通信に対する登録料金情報（課金情報）を生成し、これをメモリ１０６に格納する。この情報は、当該鍵利用者への料金請求に際して利用される。

【0055】上記の処理により、鍵利用者に秘密鍵Ｓが配布されると、鍵利用者は、秘密鍵Ｓを用いて、情報提供者との間で暗号通信を行う。あるいは、秘密鍵Ｓを用いて情報提供者との間で鍵共有を行った後に、その共有鍵により暗号通信を行う。

【0056】ここで、鍵管理者と情報提供者とが同一である場合における、鍵利用者および情報提供者間で暗号通信を行うためのシステムを図５に示す。図示するように、情報提供者装置５００は、鍵管理者装置１００により鍵利用者に配布した秘密鍵Ｓを用いて、当該鍵利用者の鍵利用者装置２００との間で、暗号通信を行う。

【0057】本実施形態では、鍵管理者は、秘密鍵Ｓを秘密情報Ｓ１、Ｓ２に分割し、秘密情報Ｓ１を記憶媒体（ＩＣカード等の計算機能付き記憶媒体を含む）に搭載してオフラインで鍵利用者に配布している。そして、秘密情報Ｓ２については、秘密情報Ｓ１および鍵利用者に付与された識別情報ＩＤを基に作成した認証情報ＡＳにより鍵利用者を認証した場合にのみ、当該鍵利用者にオンラインで送信するようにしている。

【0058】このようにすることで、たとえ、オフラインで配布した記憶媒体が不正者に盗用されたとしても、それだけでは、不正者は、秘密鍵Ｓを復元するのに必要なすべての秘密情報Ｓ１、Ｓ２を取得することができない。このため、秘密鍵情報を配布する際に、当該秘密鍵情報が不正者に横取りされる可能性を減少させることができ、ひいては、暗号通信のセキュリティを向上させることができる。

【0059】また、本実施形態において、鍵管理者装置１００は、秘密情報Ｓ１および鍵利用者に付与された識別情報ＩＤを基に作成した認証情報ＡＳにより鍵利用者が認証された場合、鍵利用者装置２００に、秘密情報Ｓ２を、秘密情報Ｓ１を鍵として暗号化して送信し、鍵利用者装置２００は、暗号化された秘密情報Ｓ２を、秘密情報Ｓ１を鍵として復号化し、復号結果と秘密情報Ｓ１とを基に、秘密鍵Ｓを復元している。このようにすることで、秘密情報Ｓ２をオンラインで送信する際のセキュリティをさらに向上させることができる。

【0060】なお、上記の実施形態では、秘密鍵Ｓを２つの秘密情報Ｓ１、Ｓ２に分割する場合について説明した。しかしながら、本発明はこれに限定されるものではなく、秘密鍵Ｓを少なくとも２つの秘密情報Ｓ１～Ｓｎ

に分割するようにしてもよい。この場合、そのうちの少なくとも1つをオフラインで配布し、残りを通信回線を使って、オンラインで送信するようにすればよい。

【0061】また、上記の実施形態では、鍵管理者装置100の課金部105により、課金情報を鍵管理者装置100内のメモリ106に格納するようにしたものについて説明したが、本発明はこれに限定されない。たとえば、課金部105を、鍵管理者装置100に設ける代わりに、鍵利用者装置200あるいは計算機能付き記憶媒体300に設け、課金情報を鍵利用者装置200内のメモリ205あるいは計算機能付き記憶媒体300内のメモリ303に格納するようにしてもよい。この情報は、鍵利用者への料金請求に際し、鍵管理者装置100に吸い上げられて利用される。

【0062】

【発明の効果】以上説明したように、本発明によれば、鍵管理者が鍵利用者に秘密鍵情報を配布する際、当該秘密鍵情報が不正者に横取りされる可能性を減少させることができ、ひいては、暗号通信のセキュリティを向上させることができる。

【図面の簡単な説明】

【図1】本発明の一実施形態である秘密鍵配布方法が適用されたシステムの概略図である。

【図2】図1に示す鍵管理者装置100の概略機能構成図である。

【図3】図1に示す鍵利用者装置200の概略機能構成図である。

【図4】図1に示す計算機能付き記憶媒体300の概略機能構成図である。

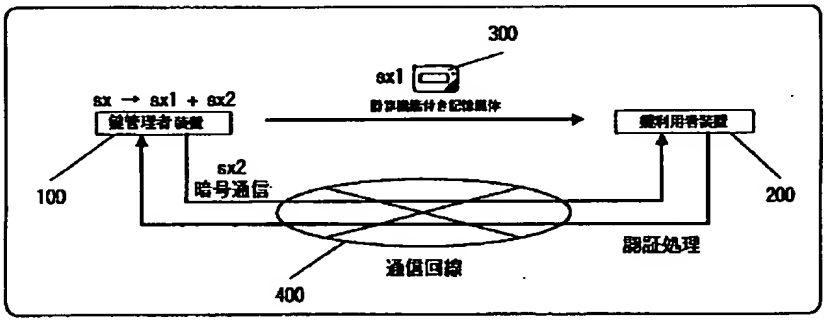
【図5】鍵管理者と情報提供者とが同一である場合における、鍵利用者および情報提供者間で暗号通信を行うためのシステムの概略図である。

【符号の説明】

100　鍵管理者装置
101、201　乱数生成部
102、203、302　演算部
103、204、301　暗復号化部
104　認証部
105　課金部
106、205、303　メモリ
107、206　通信部
200　鍵利用者装置
202　素数生成部
300　計算機能付き記憶媒体
400　通信回線
500　情報提供者装置

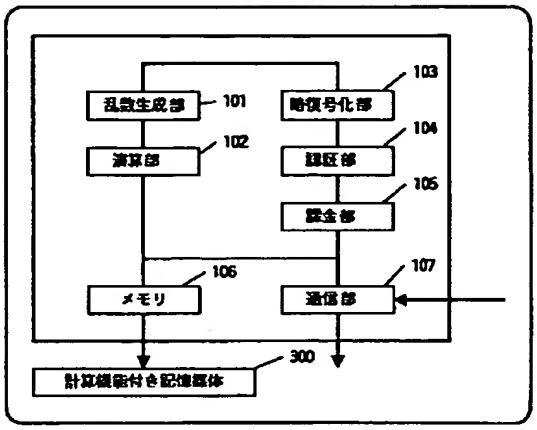
【図1】

図1



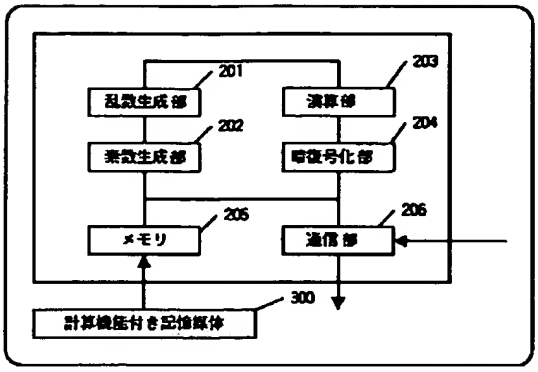
【図2】

図2



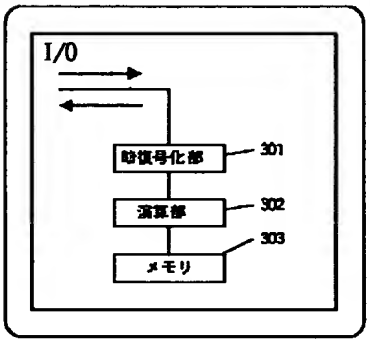
【図3】

図3



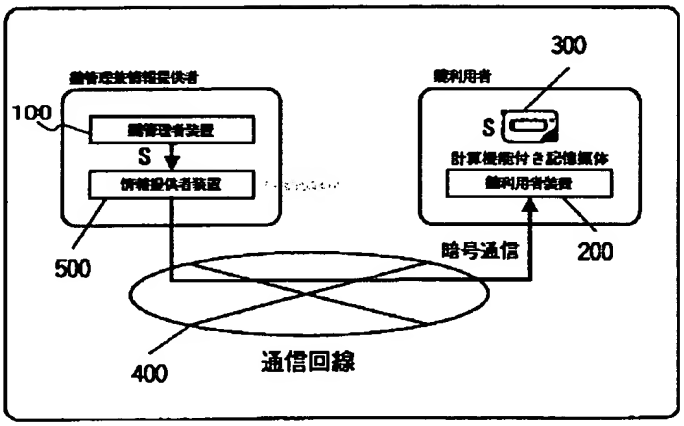
【図4】

図4



【図5】

図5



PTO 04-1462

Japanese Patent

Document No. H11-298470

Key Distribution Method and System

[Kagi Haifu Hoho oyobi Shisutemu]

Masanori Yamazaki, et al.

UNITED STATES PATENT AND TRADEMARK OFFICE

Washington, D.C. January 2004

Translated by: Schreiber Translations, Inc.

Country	:	JP
Document No.	:	H11-298470
Document Type	:	A
Language	:	Japanese
Inventor	:	Masanori Yamazaki, Genji Nishioka
Applicant	:	Hitachi Ltd.
IPC	:	H04L 9/08, H04L 9/10, H04L 9/32
Application Date	:	April 16, 1998
Publication Date	:	October 29, 1999
Foreign Language Title	:	Kagi Haifu Hoho oyobi Shisutemu
English Title	:	Key Distribution Method and System

[Claims]

[Claim 1] A key distribution method used in cryptographic communication, characterized in that it comprises:

at the key manager device:

a first step which generates a secret key S and splits that secret key S into at least two items of secret information S1-Sn ($n \geq 2$);

a second step which distributes offline to a key user at least one item of secret information Si ($1 \leq i \leq n$) of the secret information S1-Sn obtained by said first step;

at the key user device:

a third step which generates authentication information AS based on the secret information Si distributed offline by said second step and identification information ID provided in advance by the key manager, and transmits that authentication information AS to the key manager device;

at the key manager device:

a fourth step which performs authentication processing of the key user based on the authentication information AS transmitted by said third step;

a fifth step which, in the event that the key user was authenticated by said fourth step, transmits to that key user device the secret information other than the secret information Si distributed offline to that key user by said

1 Numbers in the margin indicate pagination in the foreign text.

second step, of the secret information S1-Sn obtained by said first step;

and at the key user device:

a sixth step which generates said secret key S based on the secret information Si distributed offline by said second step, and the secret information S1-Sn other than the secret information Si, which was transmitted by said fifth step.

[Claim 2] The key distribution method recited in Claim 1, characterized in that:

said fifth step, in the event that the key user was authenticated by said fourth step, transmits to that key user device the secret information other than the secret information Si distributed offline to that key user by said second step, of the secret information S1-Sn obtained by said first step, having encrypted it with said secret information Si as a key;

and said sixth step decrypts the encrypted secret information S1-Sn other than the secret information Si, which was transmitted by said fifth step, with said secret information Si as a key, and generates said secret key S based on the decryption result and said secret information Si.

[Claim 3] The key distribution method recited in Claim 1 or 2, characterized in that it further comprises:

at the key user device:

a seventh step which generates authentication information AS' based on the secret key S restored by said sixth step, and transmits that authentication information AS' to the key manager device;

at the key manager device:

an eighth step which performs authentication processing of the key user based on the authentication information AS' transmitted by said seventh step;

and at the key manager device and/or the key user device:

a ninth step which, in the event that the key user was authenticated by said eighth step, performs billing processing of a registration fee for cryptographic communication using said secret key S.

[Claim 4] A key distribution system comprising a key manager device for generating a key and a key user device for performing cryptographic communication using the key generated by that key manager device, characterized in that:

said key manager device comprises:

a key generating means which generates a secret key S and splits that secret key S into at least two items of secret information S1-Sn ($n \geq 2$);

a storing means which stores on a storage medium at least one item of secret information Si ($1 \leq i \leq n$) of the secret information S1-Sn obtained by said key generating means;

a first receiving means which receives authentication

information AS transmitted from said key user device;
an authenticating means which performs authentication processing of the key user based on the authentication information AS received by said receiving means;
and a first transmitting means which, in the event that the key user was authenticated by said authenticating means, transmits to said key user device the secret information other than the secret information Si stored on the storage medium by said storing means, of the secret information S1-Sn obtained by said key generating means;
and said key user device comprises:
a reading means which reads said secret information Si from the storage medium on which the secret information Si was stored by said key manager device;
an authentication information generating means which generates authentication information AS based on the secret information Si read by said reading means and identification information ID provided in advance by the key manager;
a second transmitting means which transmits to said key manager device the authentication information AS generated by said authentication information generating means;
a second receiving means which receives the secret information S1-Sn other than the secret information Si, which was transmitted by said key manager device;
and a key restoring means which restores the secret key S

generated by said key manager device, based on the secret information Si read by said reading means and the secret information S1-Sn other than the secret information Si, which was received by said second receiving means.

[Claim 5] A key distribution system comprising a key manager device for generating a key, a key user device for performing cryptographic communication using the key generated by that key manager device, and a storage medium with computing function, characterized in that:

said key manager device comprises:

a key generating means which generates a secret key S and splits that secret key S into at least two items of secret information S1-Sn ($n \geq 2$);

a storing means which stores on said storage medium with computing function at least one item of secret information Si ($1 \leq i \leq n$) of the secret information S1-Sn obtained by said key generating means;

a first receiving means which receives authentication information AS transmitted from said key user device;

/3

an authenticating means which performs authentication processing of the key user based on the authentication information AS received by said receiving means;

and a first transmitting means which, in the event that the key user was authenticated by said authenticating means,

transmits to said key user device the secret information other than the secret information Si stored on said storage medium with computing function by said storing means, of the secret information S1-Sn obtained by said key generating means;

said key user device comprises:

a connecting means which connects said storage medium with computing function;

a second transmitting means which transmits to said key manager device the authentication information AS output from said storage medium with computing function connected by said connecting means;

and a second receiving means which receives the secret information S1-Sn other than the secret information Si, which was transmitted from said key manager device, and outputs it to said storage medium with computing function connected by said connecting means;

and said storage medium with computing function comprises:

an authentication information generating means which generates authentication information AS based on the stored secret information Si and identification information ID provided in advance by the key manager, and outputs it to said key user device to which same medium is connected;

and a key restoring means which restores the secret key S generated by said key manager device based on the stored

secret information Si and the secret information S1-Sn other than the secret information Si, which was output from said key user device to which same medium is connected.

[Claim 6] An information processing device for distributing a key to a key user for performing cryptographic communication, characterized in that it comprises:

a key generating means which generates a secret key S and splits that secret key S into at least two items of secret information S1-Sn ($n \geq 2$);

a storing means which stores on a storage medium at least one item of secret information Si ($1 \leq i \leq n$) of the secret information S1-Sn obtained by said key generating means;

a receiving means which receives authentication information AS transmitted from the key user device, which was generated based on the secret information Si and identification information provided in advance to that key user;

an authenticating means which performs authentication processing of the key user based on the authentication information AS received by said receiving means;

and a transmitting means which, in the event that the key user was authenticated by said authenticating means, transmits to that key user device the secret information other than the secret information Si stored on the storage medium by said storing means, of the secret information S1-Sn obtained by said key generating means.

[Claim 7] The information processing device recited in Claim 6, characterized in that it further comprises an encrypting means which, in the event that the key user was authenticated by said fourth step, encrypts the secret information other than the secret information Si stored on the storage medium by said storing means, with said secret information Si as a key, and outputs to said transmitting means.

[Claim 8] The information processing device recited in Claim 6 or 7, characterized in that:

said receiving means receives authentication information AS' generated based on the secret key S, which was received from the key user device;

said authenticating means performs authentication processing based on the authentication processing AS' received by said receiving means;

and it further comprises a billing means which, in the event that the key user was authenticated by said authenticating means based on the authentication information AS', stores information of that key user specifying a registration fee for cryptographic communication using said secret key S.

[Claim 9] An information processing device for restoring a key based on secret information S1-Sn ($n \geq 2$) obtained by splitting a secret key S into at least two parts at a key manager device, characterized in that it comprises:

a reading means which reads secret information Si ($1 \leq i \leq n$) stored on a storage medium distributed by the key manager;

an authentication information generating means which generates authentication information AS based on the secret information Si read by said reading means and identification information ID provided in advance by the key manager;

a transmitting means which transmits to the key manager device the authentication information AS generated by said authentication information generating means;

a receiving means which receives the secret information S1-Sn other than the secret information Si, which was transmitted from the key manager device;

and a key restoring means which restores the secret key S based on the secret information Si read by said reading means and the secret information S1-Sn other than the secret information Si, which was received by said receiving means.

[Claim 10] The information processing device recited in Claim 9, characterized in that:

the secret information S1-Sn other than the secret information Si, which was transmitted from the key manager device, is encrypted with the secret information Si as a key;

and it further comprises a decrypting means which decrypts the encrypted secret information S1-Sn other than the secret

information Si, which was received by said receiving means, with the secret information Si read by said reading means as a key, and outputs to said key restoring means.

[Claim 11] The information processing device recited in Claim 9 or 10, characterized in that:

said authentication information generating means generates authentication information AS' based on the secret key S restored by said key restoring means;

said transmitting means transmits to the key manager device the authentication information AS' generated by said authentication information generating means;

and it further comprises a billing means which, in the event that the key user was authenticated by said authentication information AS' at the key manager device, stores information of that key user specifying a registration fee for cryptographic communication using said secret key S.

/4

[Claim 12] A storage medium with computing function constituted to as to be installable in a key user device for restoring a key based on secret information S1-Sn ($n \geq 2$) obtained by splitting a secret key S into at least two parts at a key manager device, and performing cryptographic communication using that key, characterized in that it comprises:

an authentication information generating means which

generates authentication information AS based on stored secret information Si ($1 \leq i \leq n$) and identification information ID provided in advance by the key manager, and transmits it to the key manager device via the key user device to which same medium is connected;

and a key restoring means which restores said secret key S based on the secret information Si which was stored by the key manager device, and the secret information S1-Sn other than the secret information Si, which was transmitted by the key manager device and was received via the key user device to which same medium is connected.

[Claim 13] The storage medium with computing function recited in Claim 12, characterized in that:

the secret information S1-Sn other than the secret information Si, which was transmitted from the key manager device, is encrypted with the secret information Si as a key;

and it further comprises a decrypting means which decrypts the encrypted secret information S1-Sn other than the secret information Si, which was received by said key user device to which same medium is connected, with the stored secret information Si as a key, and outputs to said key restoring means.

[Claim 14] The storage medium with computing function recited in Claim 12 or 13, characterized in that:

said authentication information generating means generates authentication information AS' based on the secret key S restored by said key restoring means, and transmits to the key manager device via the key user device to which same medium is connected;

and it further comprises a billing means which, in the event that the key user was authenticated by said authentication information AS' at the key manager device, stores information of that key user specifying a registration fee for cryptographic communication using said secret key S.

[Detailed Explanation of the Invention]

[0001]

[Field of the Invention] The present invention relates to technology for distributing keys used in cryptographic communications to users (for example, recipients of cryptographic data).

[0002]

[Prior Art] Generally, secret key cryptography is used when large volumes of data are transmitted cryptographically. In secret key cryptography, a key that is common between the sender and the recipient (common key) must be used. As methods of distribution of common keys, there are copy key schemes, individual key schemes, and the like, but in any case, conventionally, for example, the secret key information is distributed to the recipient by loading the

secret key information on an IC card, or the like, and distributing offline to the recipient, or by transmitting the secret key information to the recipient by cryptographic communication, or the like.

[0003]

[Problems the Invention Attempts to Solve] However, with the method which distributes offline by loading the secret key information on an IC card, or the like, one can imagine the possibility that an unauthorized party may steal this storage medium and impersonate the legitimate recipient. Also, with the method which transmits the secret key information by cryptographic communication, or the like, one can imagine the possibility that an unauthorized party may wiretap and crack the secret key information and impersonate the legitimate recipient.

[0004] The present invention was created in consideration of the above situation, and the purpose of the present invention is to reduce the possibility that that secret key information may be intercepted by an unauthorized party, and to improve the security of cryptographic communication.

[0005]

[Means for Solving the Problems] In order to solve the above problem, the present invention is a key distribution method used in cryptographic communication, characterized in that it comprises: at the key manager device, a first step

which generates a secret key S and splits that secret key S into at least two items of secret information S1-Sn ($n \geq 2$), and a second step which distributes offline to a key user at least one item of secret information Si ($1 \leq i \leq n$) of the secret information S1-Sn obtained by said first step; at the key user device, a third step which generates authentication information AS based on the secret information Si distributed offline by said second step and identification information ID provided in advance by the key manager, and transmits that authentication information AS to the key manager device; at the key manager device, a fourth step which performs authentication processing of the key user based on the authentication information AS transmitted by said third step, and a fifth step which, in the event that the key user was authenticated by said fourth step, transmits to that key user device the secret information other than the secret information Si distributed offline to that key user by said second step, of the secret information S1-Sn obtained by said first step; and at the key user device, a sixth step which generates said secret key S based on the secret information Si distributed offline by said second step, and the secret information S1-Sn other than the secret information Si, which was transmitted by said fifth step.

[0006] According to the present invention, the key manager

divides the secret key S into plural items of secret information S1-Sn, and distributes at least one item of secret information Si thereof to the key user offline by loading it on a storage medium (including a storage medium with computing function such as an IC card). Also, it is made such that the remainder is transmitted online to that key user only if the key user was authenticated by the authentication information AS created based on the secret information Si and the identification information ID given to the key user.

[0007] By doing thus, even if the storage medium distributed offline was stolen by an unauthorized party, with just that, it does not become the case that the unauthorized party has acquired

/5

all of the secret information S1-Sn necessary for restoring the secret key S. Likewise, even if the secret information transmitted online was wiretapped by an unauthorized party, with just that, it does not become the case that the unauthorized party has acquired all of the secret information S1-Sn necessary for restoring the secret key S. Therefore, when distributing secret key information, the possibility that that secret key information may be intercepted by an unauthorized party can be reduced, and consequently the security of the cryptographic communication

can be improved.

[0008] In the present invention, it may be that said fifth step, in the event that the key user was authenticated by said fourth step, transmits to that key user device the secret information other than the secret information Si distributed offline to that key user by said second step, of the secret information S1-Sn obtained by said first step, having encrypted it with said secret information Si as a key; and it also may be that said sixth step decrypts the encrypted secret information S1-Sn other than the secret information Si, which was transmitted by said fifth step, with said secret information Si as a key, and generates said secret key S based on the decryption result and said secret information Si.

[0009] By doing thus, the security when the secret information S1-Sn other than the secret information Si is transmitted online can be further improved.

[0010]

[Modes of Working of the Invention] A mode of working of the present invention is explained below.

[0011] Fig. 1 is a generalized drawing of a system in which the secret key distribution method being one mode of working of the present invention is applied.

[0012] As illustrated, the method of the present mode of working is implemented in a system including a key manager

device 100 and a key user device 200 which are mutually connected by a communication circuit 400, and a storage medium with computing function 300 which is constituted to be installable in the key manager device 100 and the key user device 200.

[0013] Fig. 2 shows the generalized functional configuration of the key manager device 100.

[0014] As illustrated, the key manager device 100 is constituted by a random number generation component 101, an arithmetic component 102, an encryption/decryption component 103, an authentication component 104, a billing component 105, a memory 106, and a communication component 107. This functional configuration may be realized in software by executing programs having coded the procedures for realizing each function in a computer, or it may be made such that it is realized in hardware by assembling the logic for realizing each function. In the case that it is realized in software, it also may be made such that the programs having coded the procedures for realizing each function are provided to the computer being stored on a storage medium such as a CD-ROM.

[0015] The key manager device 100 is provided with a mechanism for connecting the storage medium with computing function 300 to be distributed offline to the key user.

[0016] Fig. 3 shows the generalized functional

configuration of the key user device 200.

[0017] As illustrated, the key user device 200 is constituted by a random number generation component 201, a prime number generation component 202, an arithmetic component 203, an encryption/decryption component 204, a memory 205, and a communication component 206. This functional configuration, just as with the key manager device 100, may be realized in software by executing programs having coded the procedures for realizing each function in a computer, or it may be made such that it is realized in hardware by assembling the logic for realizing each function. In the case that it is realized in software, it also may be made such that the programs having coded the procedures for realizing each function are provided to the computer being stored on a storage medium such as a CD-ROM.

[0018] The key user device 200 is provided with a mechanism for connecting the storage medium with computing function 300 distributed offline from the key manager.

[0019] Fig. 4 shows the generalized functional configuration of the storage medium with computing function 300.

[0020] As illustrated, the storage medium with computing function 300 is constituted by an encryption/decryption component 301, an arithmetic component 302, and a memory 303. This functional configuration may be realized in

software by executing programs having coded the procedures for realizing each function in an IC card, or it may be made such that it is realized in hardware by assembling the logic for realizing each function.

[0021] Next, the secret key distribution method being the first mode of working of the present invention, which is implemented in the system explained above, is explained.

[0022] First, the key manager device 100, following instruction by the key manager, generates a random number S using the random number generation component 101 and uses this as the secret key of the key user. After that, it splits the secret key S into secret information S1 and S2 using the arithmetic component 102, and stores the secret key S and the secret information S1 and S2 in the memory 106. Next, the key manager device 100 retrieves the secret information S1 from the memory 106, and stores this in the memory 303 in the storage medium with computing function 300 connected to the key manager device 100.

[0023] The key manager distributes offline to the intended user the storage medium with computing function 300 on which is stored the secret information S1.

[0024] The key user having received the storage medium with computing function 300 on which is stored the secret information S1 connects this to the key user device 200.

[0025] The key user device 200, following instruction by

the key user, retrieves the secret information S1 from the storage medium with computing function 300, and uses the secret information S1 along with identification information ID of that key user provided in advance by the key manager in order to perform

/6

authentication processing with the key manager device 100.

[0026] There are various methods for authentication processing, but here, for example, a case when using the RSA signature scheme and a case when using the ElGamal signature scheme are explained.

[0027] First, the case when using the RSA signature scheme is explained.

[0028] The key user device 200, following instruction by the key user, creates in advance the information below using the random number generation component 201, the prime number generation component 202, and the arithmetic component 203, and stores it in the memory 205.

[0029]

[Eq. 1]

Eq. 1

- Secret information p, q: prime numbers
- Signing key (d, n), d <element> Z, n = pq
- Verification key (e, n), e <element> Z, n = pq ... (Eq. 1)

[0030] Here, the signing key is secret and the verification

key is public. The key user device 200 outputs to the storage medium with computing function 300 the signing key, and the identification information ID of that key user provided in advance by the key manager which was input by the key user. On receiving this, the storage medium with computing function 300 <text moved up from [0032]> computes the authentication information AS from

[0031]

[Eq. 2]

Eq. 2

$AS = S'^{d} \pmod{n}$ ... (Eq. 2)

[0032] <text moved down from [0030]> using the arithmetic component 302. Here, S' is a value of a prescribed function (for example, a hash value) with the secret information S1 and the identification information ID as input. Next, the storage medium with computing function 300 outputs the authentication information AS to the key user device 200. On receiving this, the key user device 200 transmits the authenticating information AS using the communication component 206 to the key manager device 100 via the communication circuit 400.

[0033] The key manager device 100, when receiving the authentication information AS by the communication component 107, <text moved up from [0035]> verifies whether or not

[0034]

[Eq. 3]

Eq. 3

$S' = AS^e \pmod{n}$ ... (Eq. 3)

[0035] is established <text moved down from [0033]> using the authentication component 104, and if it is established, it is authenticated that the key user of the key user device 200 having sent the authentication information AS is a valid user. The key manager device 100 stores in the memory 106, in correspondence, the identification information ID provided to the key user and the secret information S1 stored on the storage medium with computing function 300 distributed offline to that user.

[0036] Next, the case when using the ElGamal signature scheme is explained.

[0037] The key user device 200, on instruction by the key user, generates a prime number p using the prime number generation component 202. <text moved up from [0039]> and generates α satisfying

[0038]

[Eq. 4]

Eq. 4

$ord_p(\alpha) = p - 1$ ... (Eq. 4)

[0039] <text moved down from [0037]> using the arithmetic component 202. Also, it outputs the generated α and the prime number p to the storage medium with computing function

300. On receiving this, the storage medium with computing function 300 <text moved up from [0041]> computes y satisfying

[0040]

[Eq. 5]

Eq. 5

$y = \alpha^{S'} \pmod{p}$ ... (Eq. 5)

[0041] <text moved down from [0039]> using the arithmetic component 302, and sets the signing key as (x, α, p) and the verification key as (y, α, p). Here, S' is a value of a prescribed function (for example, a hash value) with the secret information S1 and the identification information ID as input.

[0042] Next, the key user device 200 generates a random number k relatively prime to p - 1 using the random number generation component 201, <text moved up from [0044]> and computes r satisfying

[0043]

[Eq. 6]

Eq. 6

$r = a^{k} \pmod{p}$ ... (Eq. 6)

[0044] Furthermore, it generates a suitable message m using the random number generation component 201, and outputs it to the storage medium with computing function 300 together with r, k. On receiving this, the storage medium with

computing function 300 <text moved up from [0046]> computes t satisfying

[0045]

[Eq. 7]

/7

Eq. 7

$$t = (m - S'r)k^{-1} \pmod{p - 1} \quad \ldots \text{(Eq. 7)}$$

[0046] <text moved down from [0044]> using the arithmetic component 302. Also, with (r, t) as the signature for the message m, it outputs the message m and the signature (r, s) to the key user device 200. On receiving this, the key user device 200 transmits the message m and the signature (r, s) using the communication component 206 to the key manager device 100 via the communication circuit 400.

[0047] The key manager device 100, when receiving the message m and the signature (r, s), <text moved up from [0049]> verifies whether or not

[0048]

[Eq. 8]

Eq. 8

$$\alpha^m = y^r r^t \pmod{p} \quad \ldots \text{(Eq. 8)}$$

[0049] is established <text moved down from [0047]> using the authentication component 104, and if it is established, it is authenticated that the key user of the key user device 200 having sent the message m and the signature (r, s) is a

valid user. The key manager device 100 stores in the memory 106, in correspondence, the identification information ID provided to the key user and the secret information S1 stored on the storage medium with computing function 300 distributed offline to that user.

[0050] If the key user is authenticated by the authentication processing explained above, the key manager device 100 encrypts the secret information S2 with the secret information S1 as a key using the encryption/decryption component 103. Also, it transmits the encrypted secret information S2 using the communication component 107 to the key user device 200 via the communication circuit 400.

[0051] The key user device 200, when receiving the encrypted secret information S2, outputs this to the storage medium with computing function 300. On receiving this, the storage medium with computing function 300 decrypts the encrypted secret information S2 with the secret information S1 as a key using the encryption/decryption component 301, and stores it in the memory 303. Furthermore, it restores the original key S based on the decrypted secret information S2 and the secret information S1 using the arithmetic component 302, and stores it in the memory 303.

[0052] Next, the key user device 200, following instruction by the key user, retrieves the secret key S from the storage

medium with computing function 300 and uses this secret key S to perform authentication processing by the same procedure as above with the key manager device 100.

[0053] In the case when using the RSA signature scheme, the secret key S should be used in place of S' in the above (Eq. 2) and (Eq. 3). Also, in the case when using the ElGamal signature scheme, the secret key S should be used in place of S' in the above (Eq. 5) and (Eq. 7).

[0054] If the key user is authenticated, the key manager device 100 generates registration fee information (billing information) for cryptographic communication using the secret key S for that user using the billing component 105, and stores this in the memory 106. This information is utilized on the occasion of invoicing that key user.

[0055] When the secret key S is distributed to the key user by the above processing, the key user performs cryptographic communication with an information provider using the secret key S. Or, after having performed key sharing with an information provider using the secret key S, one performs cryptographic communication using that shared key.

[0056] Here, a system for performing cryptographic communication between a key user and an information provider in the case when the key manager and the information provider are identical is shown in Fig. 5. As illustrated, the information provider device 500 performs cryptographic

communication with the key user device 200 of that user, using the secret key S distributed to the key user by the key manager device 100.

[0057] In the present mode of working, the key manager splits the secret key S into secret information S1 and S2, and distributes the secret information S1 offline to the key user being loaded on a storage medium (including a storage medium with computing function such as an IC card). Also, it is made such that the secret information S2 is transmitted online to that key user only if the key user was authenticated by the authentication information AS created based on the secret information S1 and the identification information ID given to the key user.

[0058] By doing thus, even if the storage medium distributed offline was stolen by an unauthorized party, with just that, the unauthorized party cannot acquire all of the secret information S1 and S2 necessary for restoring the secret key S. Therefore, when distributing secret key information, the possibility that that secret key information may be intercepted by an unauthorized party can be reduced, and consequently the security of the cryptographic communication can be improved.

[0059] Also, in the present mode of working, the key manager device 100, in the event that the key user was authenticated by the authentication information AS created

based on the secret information S1 and the identification information ID given to the key user, transmits the secret information S2 to the key user device 200, having encrypted it with the secret information S1 as a key, and the key user device 200 decrypts the encrypted secret information S2 with the secret information S1 as a key, and restores the secret key S based on the decryption result and the secret key S1. By doing thus, the security when the secret information S2 is transmitted online can be further improved.

[0060] In the above mode of working, a case when the secret key S was split into two items of secret information S1 and S2 was explained. However, the present invention is not limited to this, and it may be made such that the secret key S is split into

/8

at least two items of secret information S1-Sn. In this case, it should be made such that at least one item thereof is distributed offline and the remainder is transmitted online using a communication circuit.

[0061] Also, in the above mode of working, a case when it was made such that the billing information is stored in the memory 106 in the key manager device 100 by the billing component 105 of the key manager device 100 was explained, but the present invention is not limited to this. For example, it also may be made such that the billing component

105 is provided in the key user device 200 or the storage medium with computing function 300 instead of being provided in the key manager device 100, and the billing information is stored in the memory 205 in the key user device 200 or the memory 303 in the storage medium with computing function 300. This information is uploaded to the key manager server 100 for utilization on the occasion of invoicing the key user.

[0062]

[Effect of the Invention] As explained above, according to the present invention, when the key manager distributes secret key information to the key user, the possibility that that secret key information may be intercepted by an unauthorized party can be reduced, and consequently the security of the cryptographic communication can be improved.

[Brief Explanation of the Drawings]

[Fig. 1] is a generalized drawing of a system in which the secret key distribution system being one mode of working of the present invention is applied.

[Fig. 2] is a generalized drawing of the functional configuration of the key manager device 100 shown in Fig. 1.

[Fig. 3] is a generalized drawing of the functional configuration of the key user device 200 shown in Fig. 1.

[Fig. 4] is a generalized drawing of the functional configuration of the storage medium with computing function

300 shown in Fig. 1.

[Fig. 5] is a generalized drawing of a system for performing cryptographic communication between a key user and an information provider in a case when the key manager and the information provider are identical.

[Explanation of the Symbols]

100 Key manager device

101, 201 Random number generation component

102, 203, 302 Arithmetic component

103, 204, 301 Encryption/decryption component

104 Authentication component

105 Billing component

106, 205, 303 Memory

107, 206 Communication component

200 Key user device

202 Prime number generation component

300 Storage medium with computing function

400 Communication circuit

500 Information provider device

図1

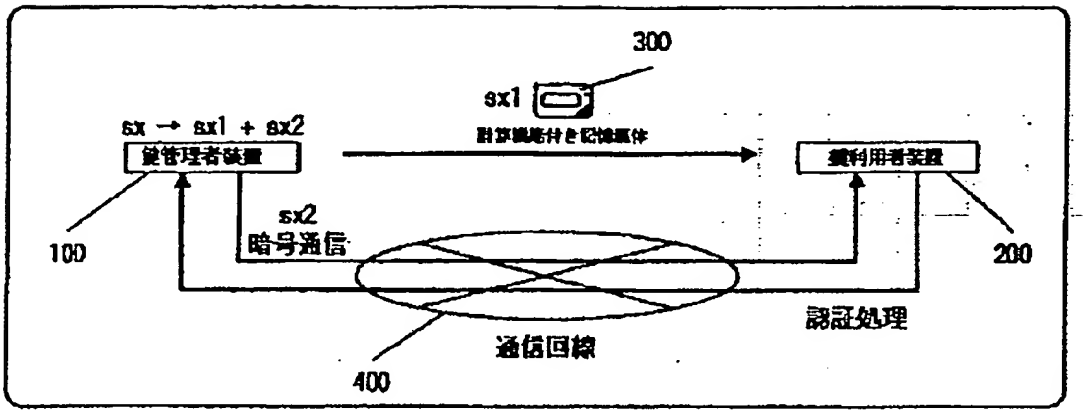


Fig. 1

100 Key manager device

200 Key user device

100 -> 200 -> 400 Cryptographic communication

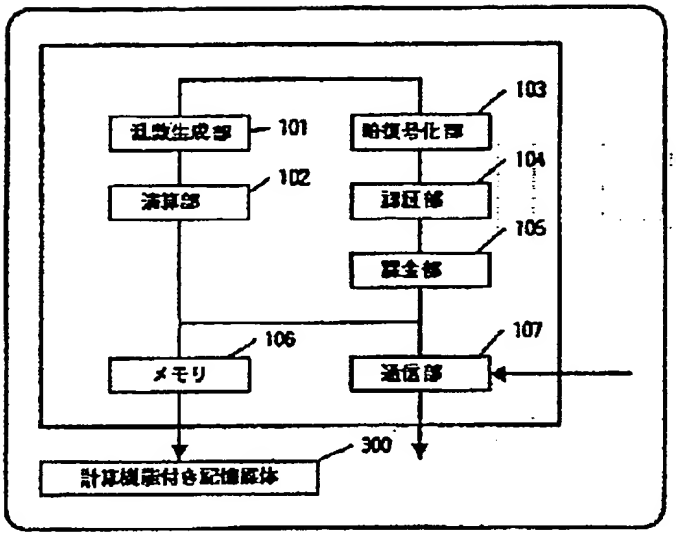
200 -> 100 -> 400 Authentication processing

300 Storage medium with computing function

400 Communication circuit

/9

図2



101 Random number generation component

102 Arithmetic component

103 Encryption/decryption component

104 Authentication component

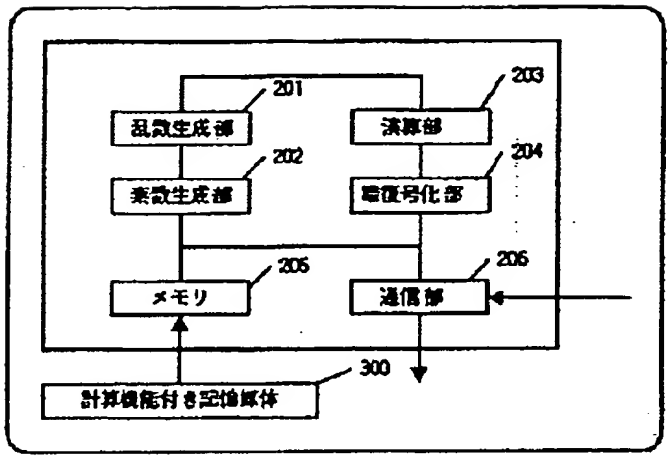
105 Billing component

106 Memory

107 Communication component

300 Storage medium with computing function

図3



201 Random number generation component

202 Prime number generation component

203 Arithmetic component

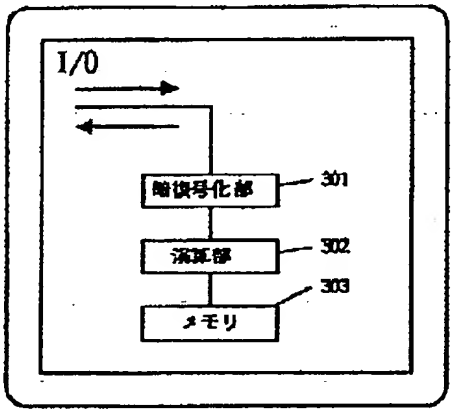
204 Encryption/decryption component

205 Memory

206 Communication component

300 Storage medium with computing function

図4

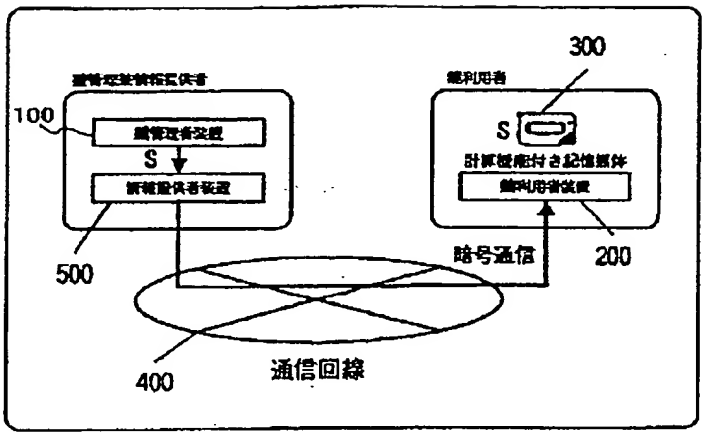


301 Encryption/decryption component

302 Arithmetic component

303 Memory

図5



100 Key manager device

200 Key user device

400 Communication circuit

500 Information provider device

<above left box> Key manager/information provider

<above right box> User

<below right box> Cryptographic communication